1343191

THE UNITED STATES OF AMERICA

TO ALL TO WHOM THESE PRESENTS SHALL COME:

UNITED STATES DEPARTMENT OF COMMERCE

United States Patent and Trademark Office

July 12, 2005

THIS IS TO CERTIFY THAT ANNEXED HERETO IS A TRUE COPY FROM THE RECORDS OF THE UNITED STATES PATENT AND TRADEMARK OFFICE OF THOSE PAPERS OF THE BELOW IDENTIFIED PATENT APPLICATION THAT MET THE REQUIREMENTS TO BE GRANTED A FILING DATE.

APPLICATION NUMBER: *60/523,685*
FILING DATE: *November 21, 2003*
RELATED PCT APPLICATION NUMBER: *PCT/US04/38907*

Certified by

Jon W. Dudas

Under Secretary of Commerce
for Intellectual Property
and Director of the United States
Patent and Trademark Office

PROVISIONAL APPLICATION FOR PATENT COVER SHEET

This is a request for filing a PROVISIONAL APPLICATION FOR PATENT under 37 CFR 1.53(b)(2).

INVENTOR(s)/APPLICANT(s)		
Given Name (first and middle [if any])	Family Name or Surname	Residence (CITY AND EITHER STATE OR FOREIGN COUNTRY)
Kenneth Donna Paul	DANCKAERT DANCKAERT DANCKAERT	Severna Park, MD Severna Park, MD Arnold, MD

☐ Additional inventors are being named on the ___ separately numbered sheets attached hereto.

TITLE OF THE INVENTION (280 characters max)

SECURE DATA AND APPLICATION MOBILITY DEVICE

CORRESPONDENCE ADDRESS

☒ Customer Number: **6449**

☐ Firm or Individual Name	Rothwell, Figg, Ernst & Manbeck, P.C.				
Address	1425 K Street, N.W.				
Address	Suite 800				
City	Washington	State	D.C.	ZIP	20005
Country	U.S.A.	Telephone	202-783-6040	Fax	202-783-6031

ENCLOSED APPLICATION PARTS *(check all that apply)*

☒ Specification *Number of Pages* [14] ☐ CD(s), Number ___
☐ Drawing(s) *Number of Sheets* [ ] ☐ Other *(specify)* ___
☐ Application Data Sheet. See 37 CFR 1.76

METHOD OF PAYMENT OF FILING FEES FOR THIS PROVISIONAL APPLICATION FOR PATENT *(check one)*

☐ Applicant claims small entity status. See 37 CFR 1.27 — Filing Fee Amount: $160.00
☐ A check or money order is enclosed to cover the filing fee
☒ The Commissioner is hereby authorized to charge filing fees or credit any overpayment to Deposit Account Number: 02-2135
☐ Payment by credit card. Form PTO-2038 is attached.

The invention was made by an agency of the United States Government or under a contract with an agency of the United States Government.

☒ No.

☐ Yes, the name of the U.S. Government agency and the Government contract number are: ___

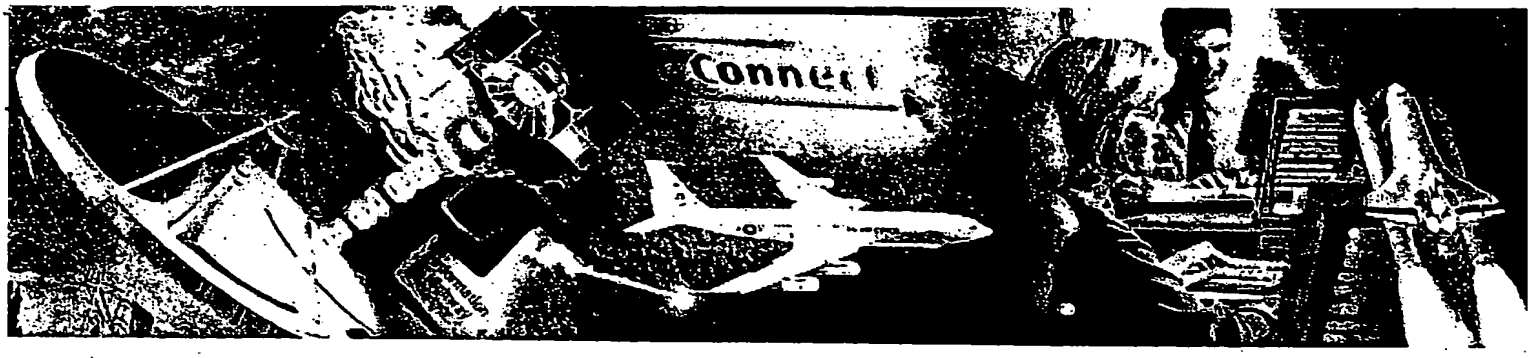
Respectfully submitted,

SIGNATURE Vincent M DeLuca Date 21 NOV 03

TYPED or PRINTED NAME Vincent M. DeLuca
TELEPHONE : 202-783-6040

REGISTRATION NO. 32,408
Docket Number: 2592-107

USE ONLY FOR FILING PROVISIONAL APPLICATION FOR PATENT



Mobile Crypto Device

The Mobile Crypto Device provides Secure Data & Application Mobility by providing secure storage, access and transport for your sensitive files on a small, easy to use USB memory device. It also provides secure, remote access to your server applications.

Secure Storage

- On device software cryptography for encryption
- On device storage and transport for both encrypted and unencrypted data
- On device certificates for authentication to the Public Key Infrastructure
- On device passwords for easy retrieval and use
- On device key storage for security and ease of use
- File scan to minimize security risks from temporary files left by applications.

Application & Data Mobility

- Encrypted file transport & Email storage
- Email verification with signature
- Windows terminal services for remote access to server applications

Acountability

- Web access control based on user needs
- LAN access control for differing access levels
- Logging to support traceability and records for tracking
- Audit logging for monitoring user actions

Authentication

- Consumer Authentication server for authentication in non-PKI environments
- LDAP server for directory services

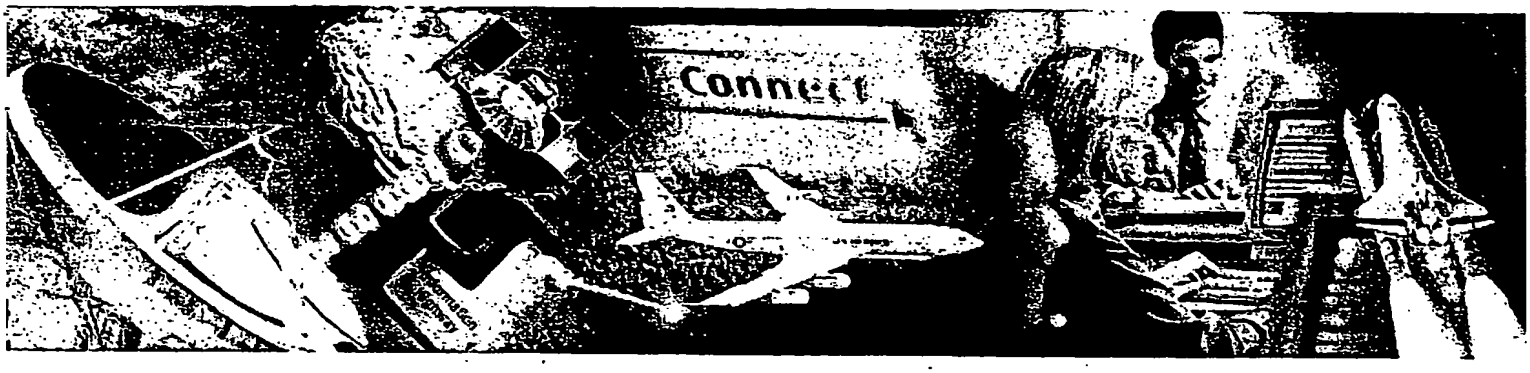
Enterprise Services & Interoperability

- Certificate issuance and revocation
- Centralized key recovery for lost or stolen keys
- File recovery for files on lost USB device
- Automated data back-up on a central server

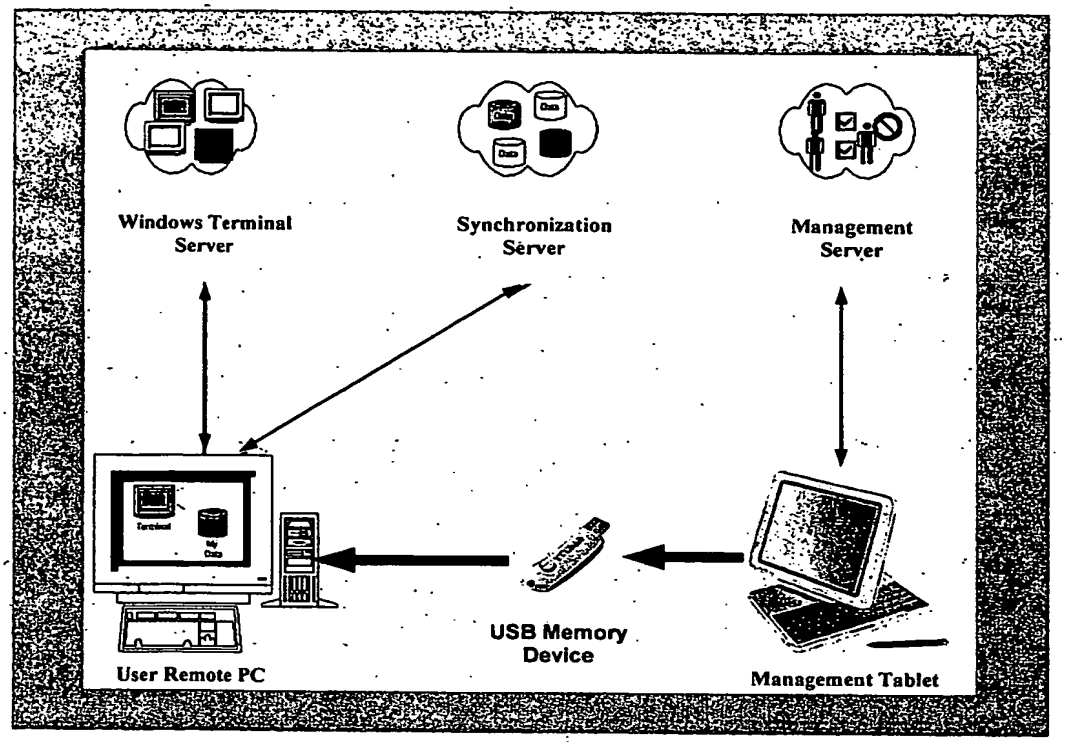
TITAN

Information Security Systems Division (ISSD)
7480 Candlewood Road • Hanover, MD • 21076
Phone: (410)694-4900 • www.titanissd.com

TITAN ISSD provides a full range of products and services to support your secure communication needs.



Mobile Crypto Device



Secure storage, transport and use of sensitive data is critical in the Government's fight against terrorism and the Titan Mobile Crypto Device provides a cost effective solution.

Technical Specifications

- 256 MB storage
- Supports Windows 2000 and Windows XP
- AES 128 bit Encryption
- Microsoft Windows Terminal Services
- Onboard Sync Application & Terminal Applications installed
- No pre-installed software

Server Requirements

- Windows 2000 Professional
- SOAP
- Open SSL
- Open LDAP

Future Capabilities

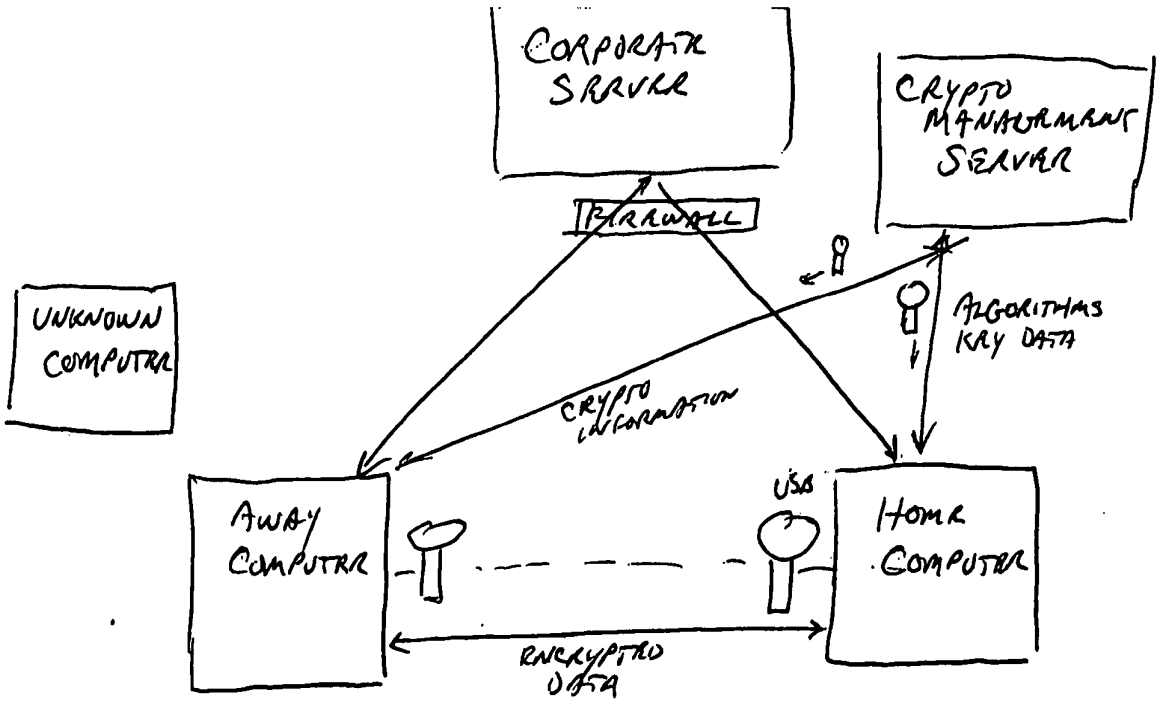
- Key Recovery
- Secure backup & recovery
- Secure Collaboration
- Virus Security Scanning
- Biometric authentication
- Authentication with the "Secure ID" Card
- Configure system security policy
- Encrypted Email

U.S. Department of Homeland Security

TITAN

nformation Security Systems Division (ISSD)
7480 Candlewood Road • Hanover, MD • 21076
Phone: (410)694-4900 • www.titanissd.com

TITAN ISSD provides a full range of products and services to support your secure communication needs.



3

ENCRYPT & STORE (IN COMPUTER OR SERVER)
ENCRYPT & STORE (ON USB STICK)
ENCRYPT & TRANSFER TO REMOTE COMPUTER
ENCRYPT & TALK TO REMOTE COMPUTER
REMOTE ACCESS TO HOME DESKTOP

VIRUS SCANNING
SECURE CLEAN UP AFTER USE
SECURITY STATUS
VULNERABILITY SCANNING (SPYWARE, ETC
FIREWALL

PASSWORD PROTECTED
BIOMETRIC ACCESS CONTROL
FILE RECOVERY
KEY RECOVERY
BACK UP & CLONE

Mobile Crypto Device (MCD) Data Flow Diagrams

The Mobile Crypto Device is designed for the secured management and replication of files, applications, and other user data. The device is based around a removable memory device that is used on an end user computer for file and data storage. The device is pre-installed with management software to secure (encrypt) and replicate/synchronize these files with a remote server.

Scenario 1: Memory Device Issuing

The process of issuing a memory device to an end user initializes the device and installs applications according to the enterprises configuration and requirements. This installation is processed by a management station, which in turn communicates with a centralized server.

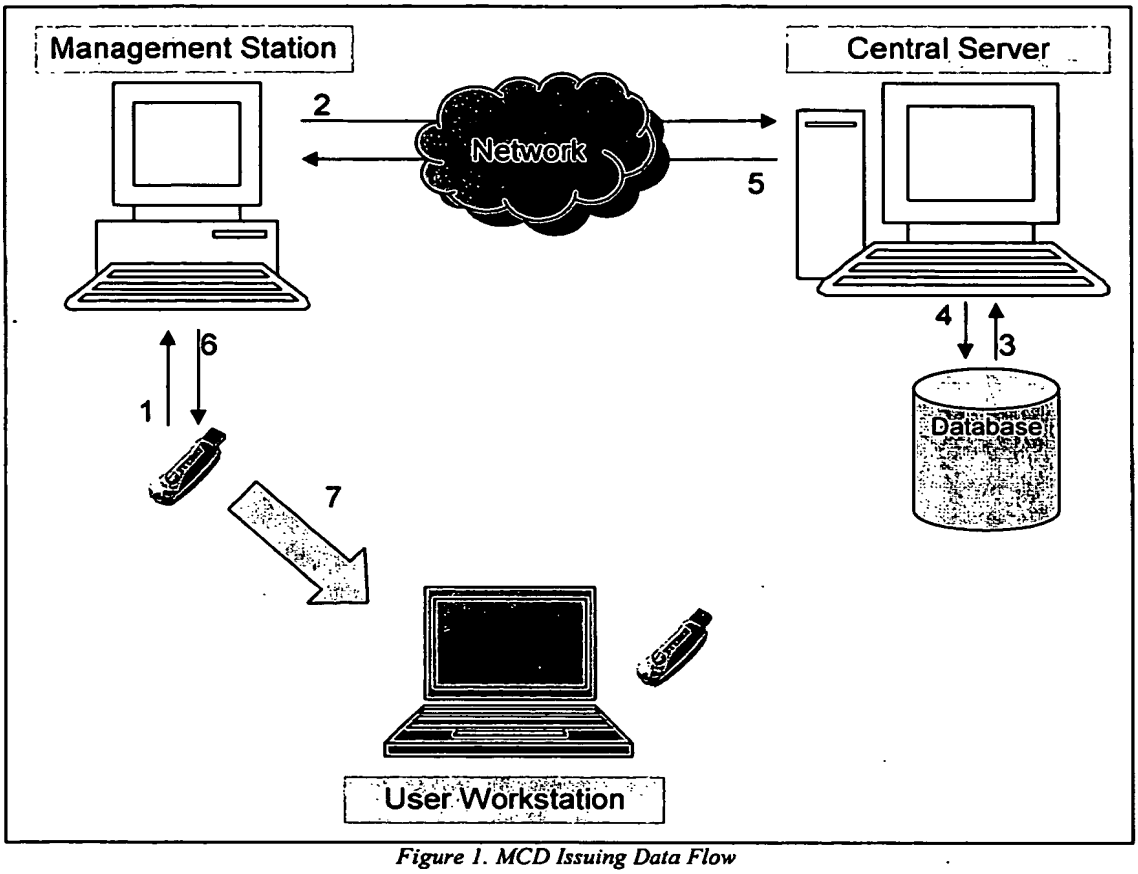


Figure 1. MCD Issuing Data Flow

Step 1: Memory Device inserted into management station

The management station will read the current state of the Memory Device, and if it is a clean device will prepare to install and configure for a new user.

Step 2: Device issue request is sent to central server

The management station will enter details to identify the user who is receiving the Memory Device and will send this information to the central server. This ensures that all users are centrally managed and that each device can be individually detailed.

Step 3: User details are read from the central directory/database

The information for the specified user is read from the centralized database. This information is used to generate appropriate keys/certificates for the user, or to identify an error in the event that the user is unknown or has a pre-existing key.

Step 4: Given a valid request, the new user details are written to the centralized database

If the request is processed correctly, the new key/certificate and issuing details are written to the centralized directory/database.

Step 5: A response is returned to the management station

A successful request or error response is returned to the management station. If the request was successful, appropriate key information is returned for storage on the memory device. If the request failed, error message details are returned.

Step 6: Device initialization

For a valid request, the memory device is now initialized. The memory is cleared and software is installed for data management and synchronization. The users details, configuration settings, and keys/certificates are written to the device, and an initial encryption of these details occurs.

Step 7: User issuing

The device is now physically issued to the end user.

Scenario 2: Memory Device Synchronization

As the user works with data on the MCD, they will synchronize with the central server at periodic intervals to ensure that all data is appropriately backed up and safe. This synchronization process occurs over a secured connection, and will synchronize all sensitive and encrypted data.

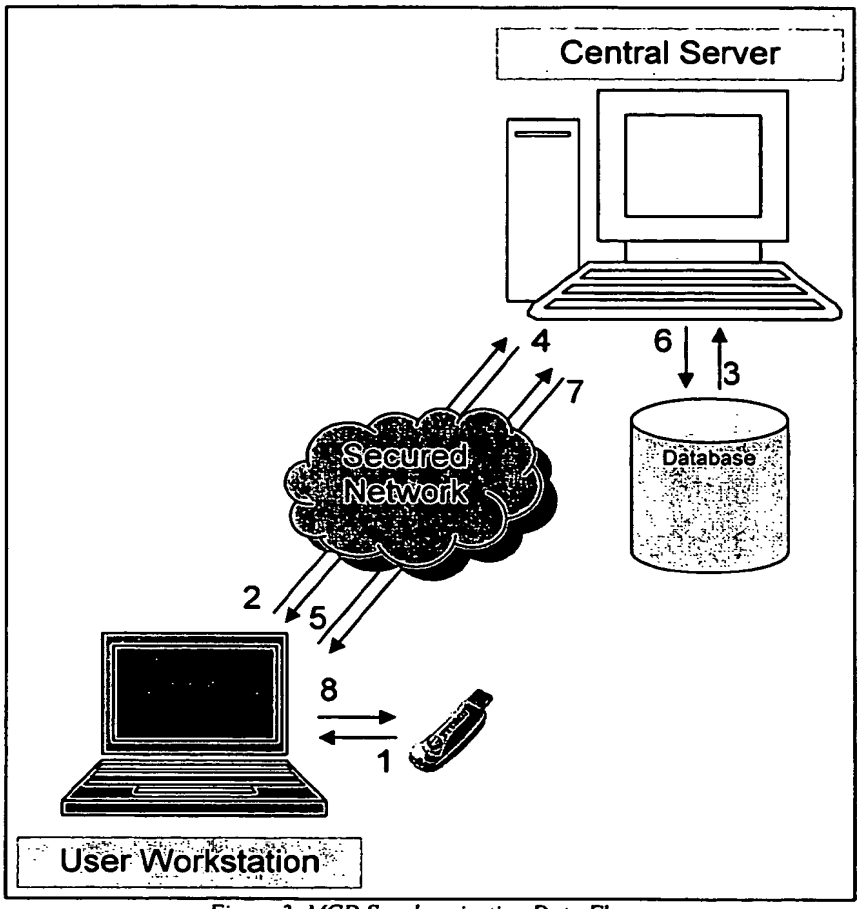


Figure 2. MCD Synchronization Data Flow

Step 1: User reads current file information from MCD

The user selects the option to synchronize files on the MCD. This will cause the MCD application to read in information on all encrypted and sensitive files from the MCD.

Step 2: User sends file information in a request to the central server

The MCD application will authenticate to the repository and send current file information to the central server as a synchronization request.

Step 3: Server reads current file state from data repository

The central server will retrieve details on the last known state of the users files that are stored in the repository. This information is then matched up with the user-sent information to determine which files have changed and need to be updated on the central server.

Step 4: Server sends file state to user workstation

The server sends a list of files that need to be sent to the server in order to fully synchronize the device as a response to the initial request.

Step 5: User sends updated files from MCD to central server

The user will sent to the central server all files detailed in the response directly from the MCD to the central server.

Step 6: Server writes updated file to data repository

The server writes all new/changed files to the server. If a file was changed, the old file is retained according to corporate data retention policies.

Step 7: Central server returns results to user

After all files have been correctly synchronized, the server returns these details to the user.

Step 8: User updates file information on MCD

The MCD application will then update the local MCD to track last synchronization details.

Scenario 3: Memory Device Application Access

As the user works with data on the MCD, they will synchronize with the central server at periodic intervals to ensure that all data is appropriately backed up and safe. This synchronization process occurs over a secured connection, and will synchronize all sensitive and encrypted data.

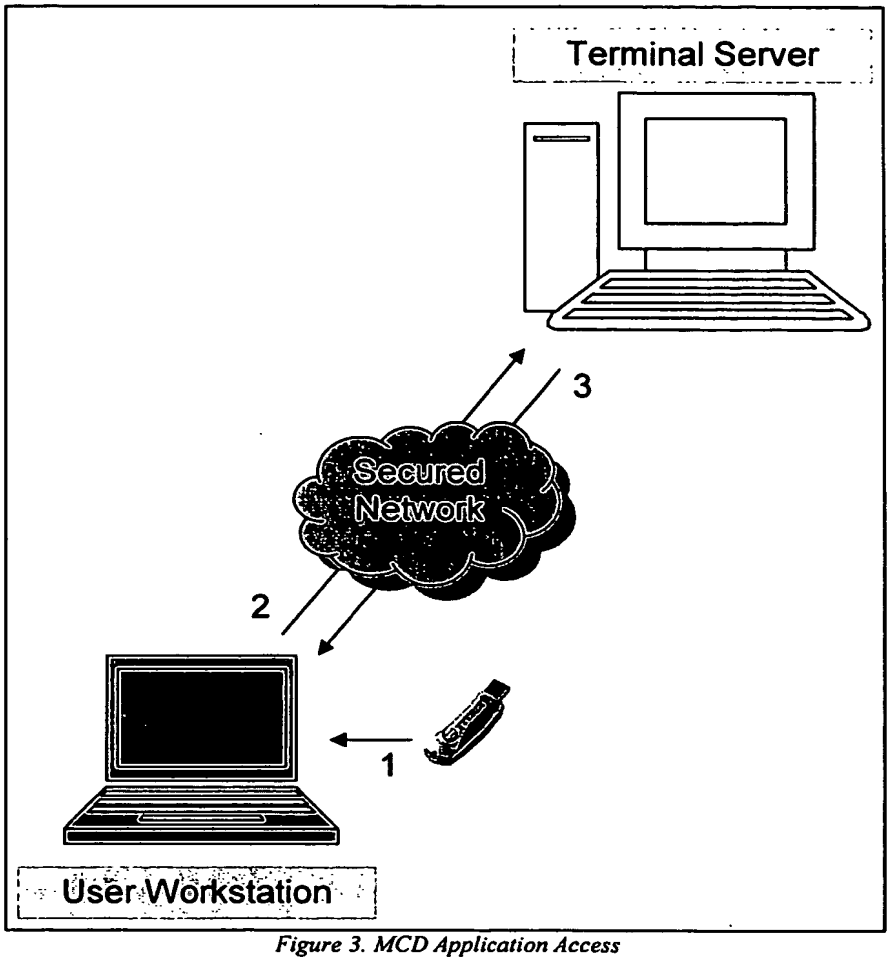


Figure 3. MCD Application Access

Step 1: User runs application access application from MCD

The user selects the remote application access function from the MCD. Reading any necessary keys/certificates from the MCD, the application executes.

Step 2: Application access application connects to corporate terminal server

The application will establish a secured connection with the corporate terminal server, passing any keys/certificates, and allowing the user to enter any other necessary authentication credentials.

Step 3: Terminal server establishes authenticated and secure connection

Upon a valid authentication, the terminal server will establish a fully connected session and allow the user to start executing applications as necessary.

IR&D Provisional Patent Application - MCD

Statement - MCD Overview

The Mobile Crypto Device (MCD) provides three main secure capabilities. The first is "Mobile Device-based Secured Data Synchronization and Exchange", which is the secured synchronization process between the MCD and the repository server. The second is "Mobile Device-based Application Access Capability", which is the act of accessing a remote software application (terminal server, for example) through software wholly contained on the MCD device. The third capability is "Mobile Device-based Security Auditing Capability", which encompasses the security features of the MCD including local vulnerability scanning, system state assessment, and other features.

1. Common Claims for each capability

1. A secure data management and remote application access device based on custom software comprising: a removable media device that holds applications, configuration information, and user data; a data management application that provides for file encryption and decryption; a data management application that allows for remote storage of user data; a data management application that allows for remote synchronization of user data; a data management application that is integrated into corporate or commercial security solutions; a data management application that is integrated into corporate or commercial Public Key Infrastructures (PKI); a data management application that is integrated into corporate and/or commercial directories; a data management application that provides for data encryption to multiple recipients; a data management application that validates that host computers have removed traces of user data from the system; an application access application that provides pre-configured remote application access executing from a removable memory device; a security application based on a removable memory device that will verify a host computing device is free of virus activity; a security application based on a removable memory device that will verify a host computing device is free of user monitoring software; a security application based on a removable memory device that will summarize host computing device security state easily for a user; a security application based on a removable memory device that will verify that all user data has been removed from a host computing device.

2. A removable memory device according to claim 1, such as a static memory device with a built-in USB interface, wherein custom software is contained in, and executed by a host computing device.

2. Mobile Device-based Secured Data Synchronization and Exchange Capability

1. A secured data management application according to claim 1, that provides a user interface to encrypt, decrypt, and manage data on behalf of a user.

2. A secured data management application according to claim 1 that enables user data and information to be securely stored on a remote server, after a successful user authentication process.

3. A secured data management application according to claim 1 that enables user data and information to be securely synchronized with previous user data on a remote server, after a successful user authentication process.

4. A secured data management application according to claim 1 that verifies that all user sensitive data that has been stored as temporary files have been removed from a host computing device.

5. A secured data management application according to claim 1 that is integrated into corporate security infrastructures and PKI systems to utilize corporate or commercially issued Keys and Certificates to encrypt and decrypt user data.

6. A secured data management application according to claim 1 that provides an inherent ability to search corporate and/or commercial directories, automatically retrieve encryption information about the user, such as public keys, and using this information to encrypt information for one or more destination users.

3. Mobile Device-based Application Access Capability

1. A remote application access application according to claim 1 that is pre-configured and installed on the removable memory device and provides a user remote access to software applications and desktop environments located on other systems, including corporate or other commercial systems.

4. Mobile Device-based Security Auditing Capability

1. A security application according to claim 1 that will operate by executing via the removable memory device and will scan and verify that a host computing device is free of virus activity.

2. A security application according to claim 1 that will operate by executing via the removable memory device and will scan and verify that a host computing device is free of user monitoring, keystroke logging, and other invasive activity.

3. A security application according to claim 1 that will operate by executing via the removable memory device and scan various aspects of a host computer and use this information to generate an easily understandable report on the state of the host system security. This security summary may be used to restrict the activities

of the user on the host to ensure that sensitive information is not exposed on an insecure or un-trusted host computer.

Method Claim:

There are three ways the Mobile Crypto Device can be fielded and deployed.

1. Initially, Titan will want to simplify the deployment of the product and its supporting infrastructure to encourage trials tests and simplify adoption. In this case, Titan will provide a hosted service. The enterprise would simply have a management application to create/manage accounts, and that all server and storage infrastructure would be maintained by a central, off-site entity. This could be provided on a user-by-user basis in order to get potential clients using the software quickly in a trial mode with little start-up effort.

2. The next method of deployment would be to use an appliance configuration. A computer will pre-configured with an operating system and Titan server software and can be installed onto a corporate network. With this approach, local (client) IT staff would have very little work to do and the capability can be up and running in even a small company very quickly. If required, Titan could provide the necessary professional IT services.

3. Ultimately, Titan envisions an enterprise version of the product that ties into corporate certificate infrastructures and directories. This method would apply to larger entities with knowledgeable IT staffs.

Document made available under the Patent Cooperation Treaty (PCT)

International application number: PCT/US04/038907

International filing date: 19 November 2004 (19.11.2004)

Document type: Certified copy of priority document

Document details: Country/Office: US
Number: 60/523,685
Filing date: 21 November 2003 (21.11.2003)

Date of receipt at the International Bureau: 15 July 2005 (15.07.2005)

Remark: Priority document submitted or transmitted to the International Bureau in compliance with Rule 17.1(a) or (b)

World Intellectual Property Organization (WIPO) - Geneva, Switzerland
Organisation Mondiale de la Propriété Intellectuelle (OMPI) - Genève, Suisse